RSAC 2025 Conference

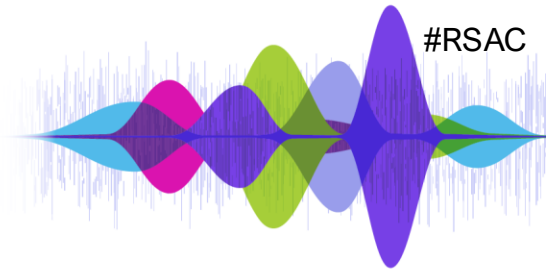
Many Voices. One Community.

SESSION ID: CSO-R02

# The Frugal CISO: Running a Strong Cybersecurity on a Budget

**Anand Thangaraju**

Field CISO – West Region
ePlus Inc.
https://www.linkedin.com/in/athangaraju/



# Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

The opinions expressed in this presentation and on the following slides are solely mine and not necessarily those of ePlus. You are free to disseminate this presentation for knowledge sharing purposes only. I do not endorse any vendors mentioned in the presentation.

# About me

- Cyber Evangelist, Practice and Channel Sales Leader
- Board Advisor & Angel for Startups. Scout and Advisor for VCs
- Prior Corporate roles at Cognizant, JPMC, EY, SVB, Zelle
- Board Member at ISACA SV Chapter and member of many communities
- Working Group Author at NIST, OWASP AI Exchange, CSA AI Governance.
- 40+ Certifications (ORM, CERP, CISA, CISSP, CIPM, SCR Professional

Anand Thangaraju
*Field CISO – West*
*ePlus Inc.*

*ePlus Inc.*

# Cybersecurity on a Budget

## Why It's More Relevant Than Ever

**Economic Constraints -** In 2023, **70% of CISOs** reported budget constraints as a primary challenge in meeting cybersecurity objectives. *(Source: Gartner)*

**Board Accountability - 88% of boards now view cybersecurity as a business risk rather than an IT issue**, demanding clearer ROI and measurable outcomes. *(Source: PwC 2024 Global Digital Trust Insights)*

**Operational Efficiency -** Enterprises use an average of **76 security tools**, yet **53% of security leaders** say this complexity weakens security posture rather than strengthens it. *(Source: IBM Security X-Force)*

**Focus on Innovation - 61% of CISOs** say security budgets compete with investments in digital transformation, AI, and cloud initiatives.
*(Source: IDC Security Survey 2023)*

The global cost of cyberattacks will be about

**$10.5 Trillion**

**Annually By 2025**

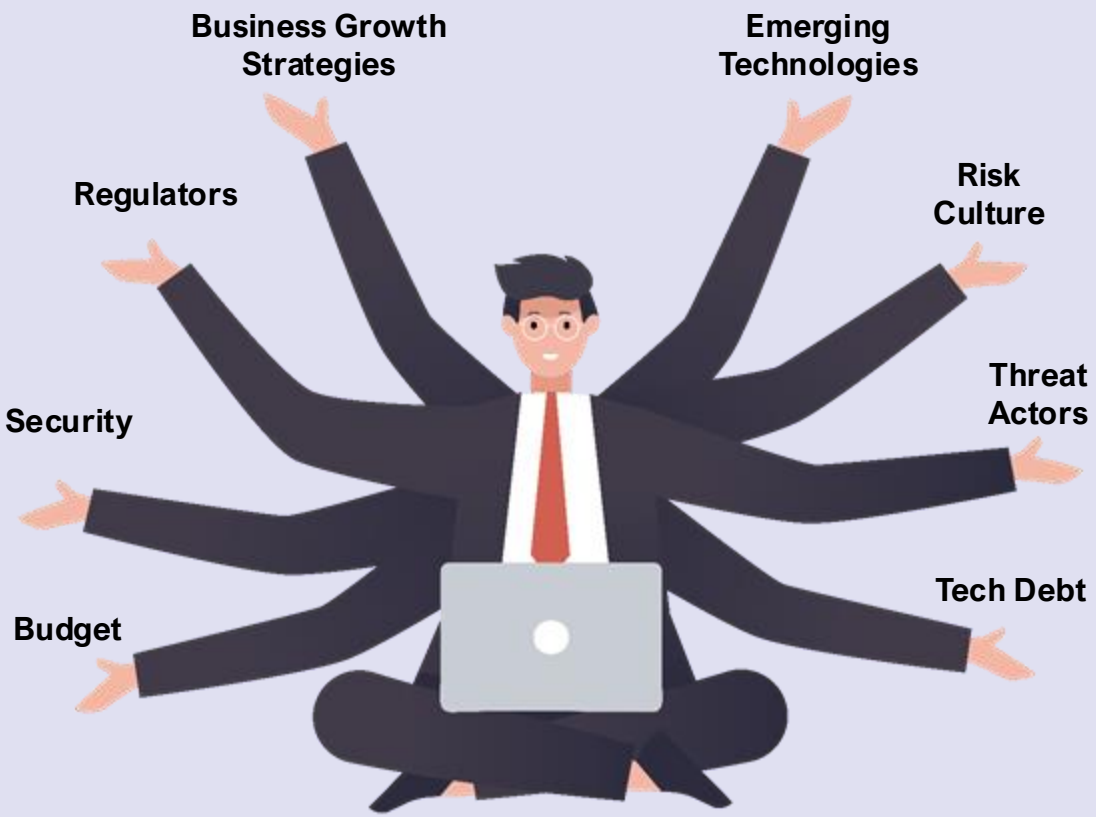
*(Source: Cybersecurity Ventures)*

Ransomware payments increased 15% from 2023

**$813 Million**

# What does it mean to be a Frugal CISO?

## The Frugal CISO



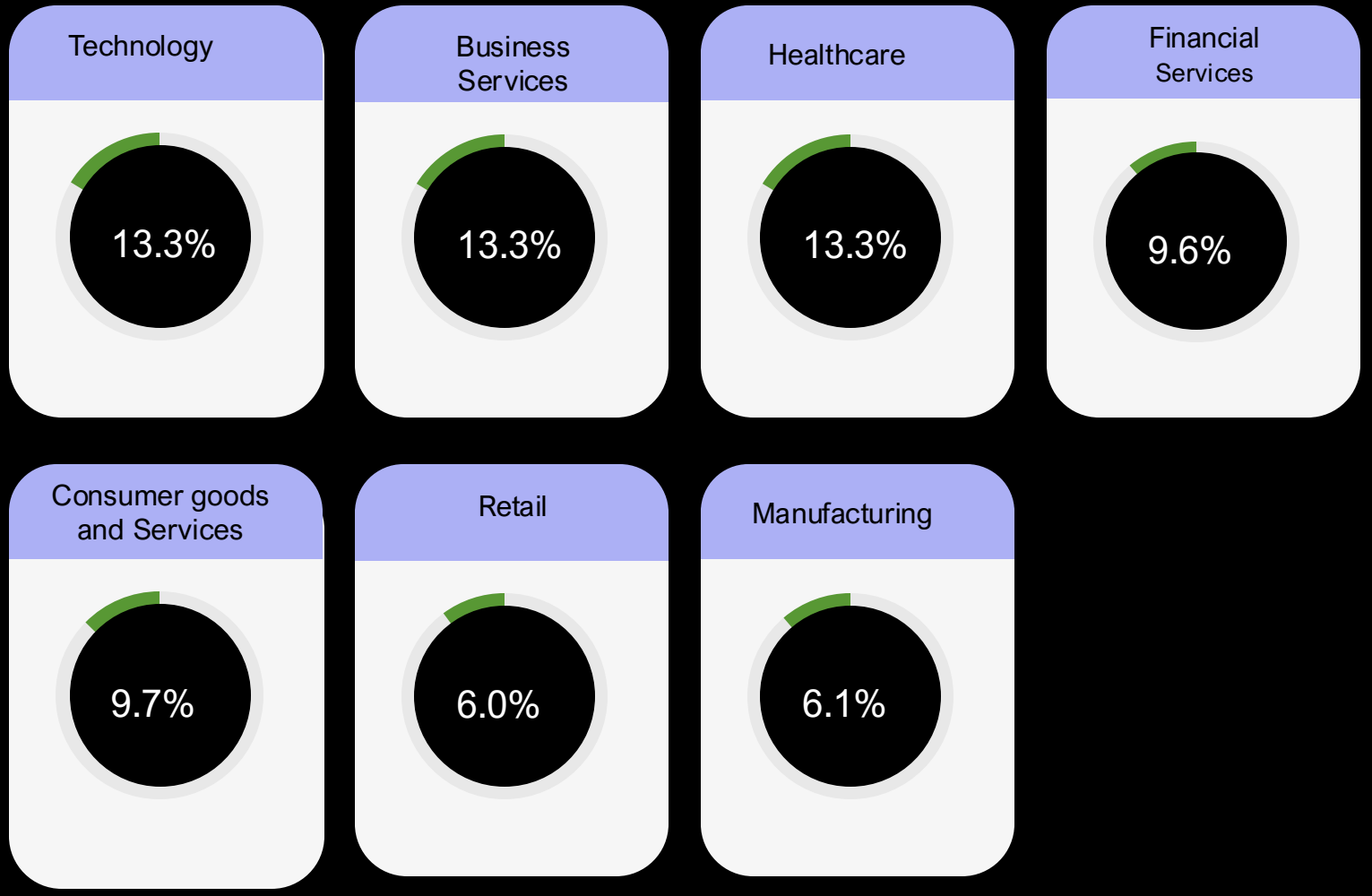
# Do we have the right number?

On an average, businesses **spend approximately 11%** of their IT budgets
on security. This is by far the easiest and most dangerous way to simplify budgeting process.

Other popular heuristics:

- Historical Trend (% increase on last year)
- % of Business Revenue
- % Cost of Non-Compliance
- % Cost of a Data Breach, given a probability of breach
- Risk based budgeting
- Industry Benchmarking
- Per-Capita Spend
- Project based funding
- Cyber Insurance Offset

Percentage of budgets spent on security by industry




Sources : 2024 Security Budget Benchmark Report: Key Findings - IANS & Artico Research

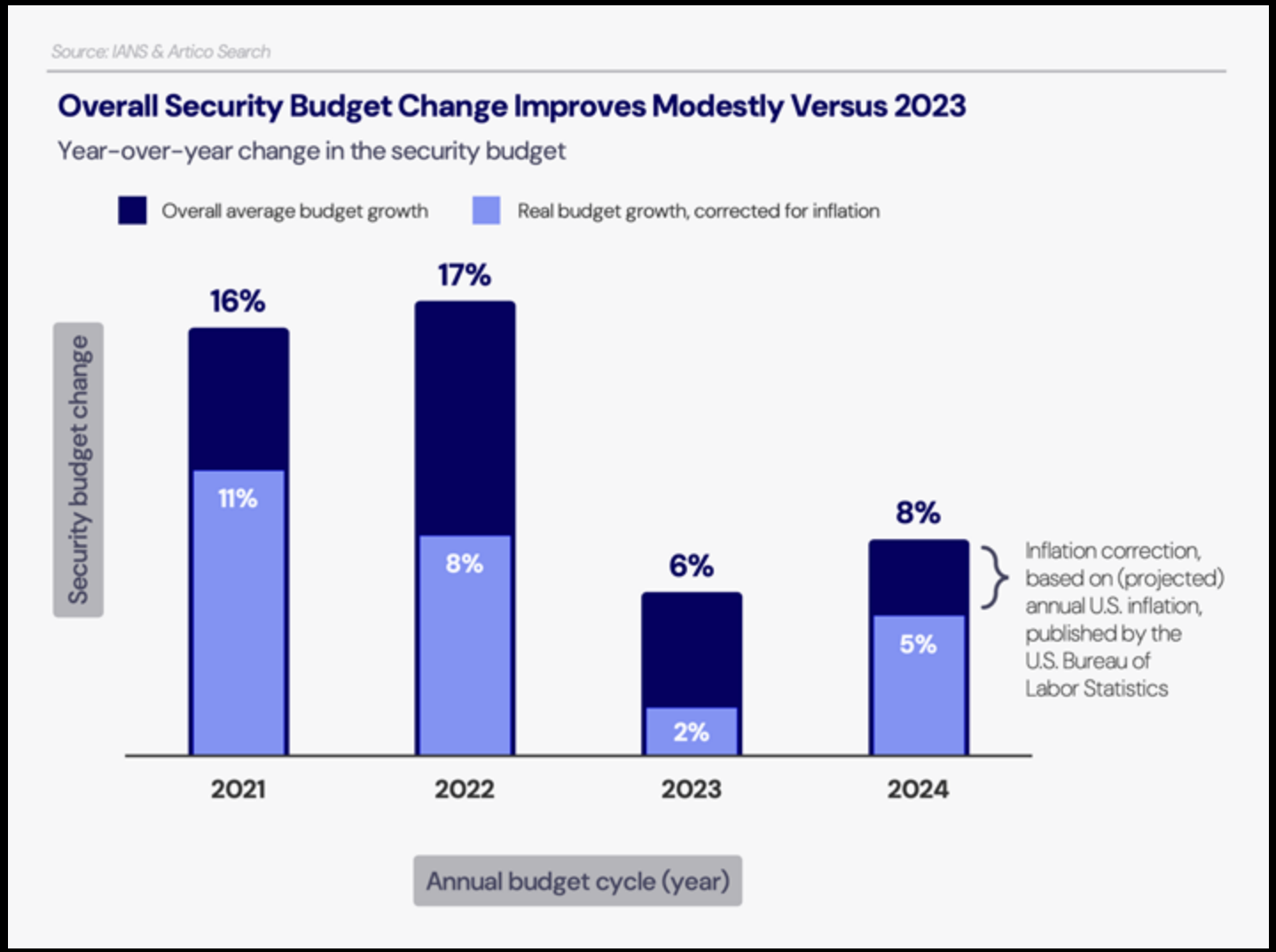
# Security Budgets

## *A recent Study*

The period of double-digit growth in security budgets seen in 2021/22 has not returned. During those years, many organizations were rapidly evolving due to the Covid induced remote work environment and uncertain business climate.

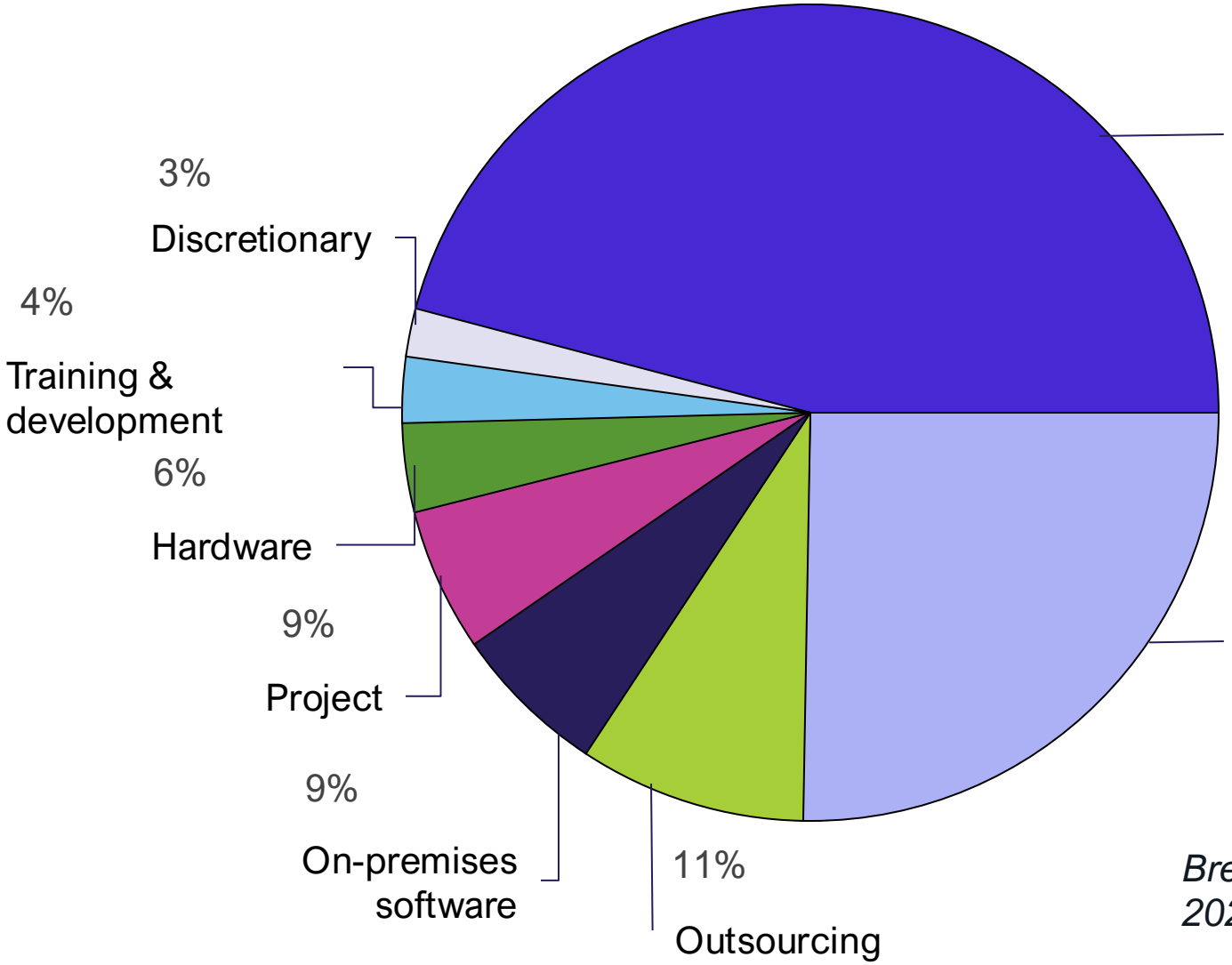
For 2024, the overall growth rate is 8%, an improvement from 2023 but still around half of 2021 and 2022 levels. When adjusted for inflation, the real growth rate for security budgets is around 5%, up from 2% in 2023 (according to the Bureau of Labor Statistics' Consumer Price Index).

## Security Budget Hyper Growth Has Ended




Sources : 2024 Security Budget Benchmark Report: Key Findings - IANS & Artico Research

# Cybersecurity Spend Priorities

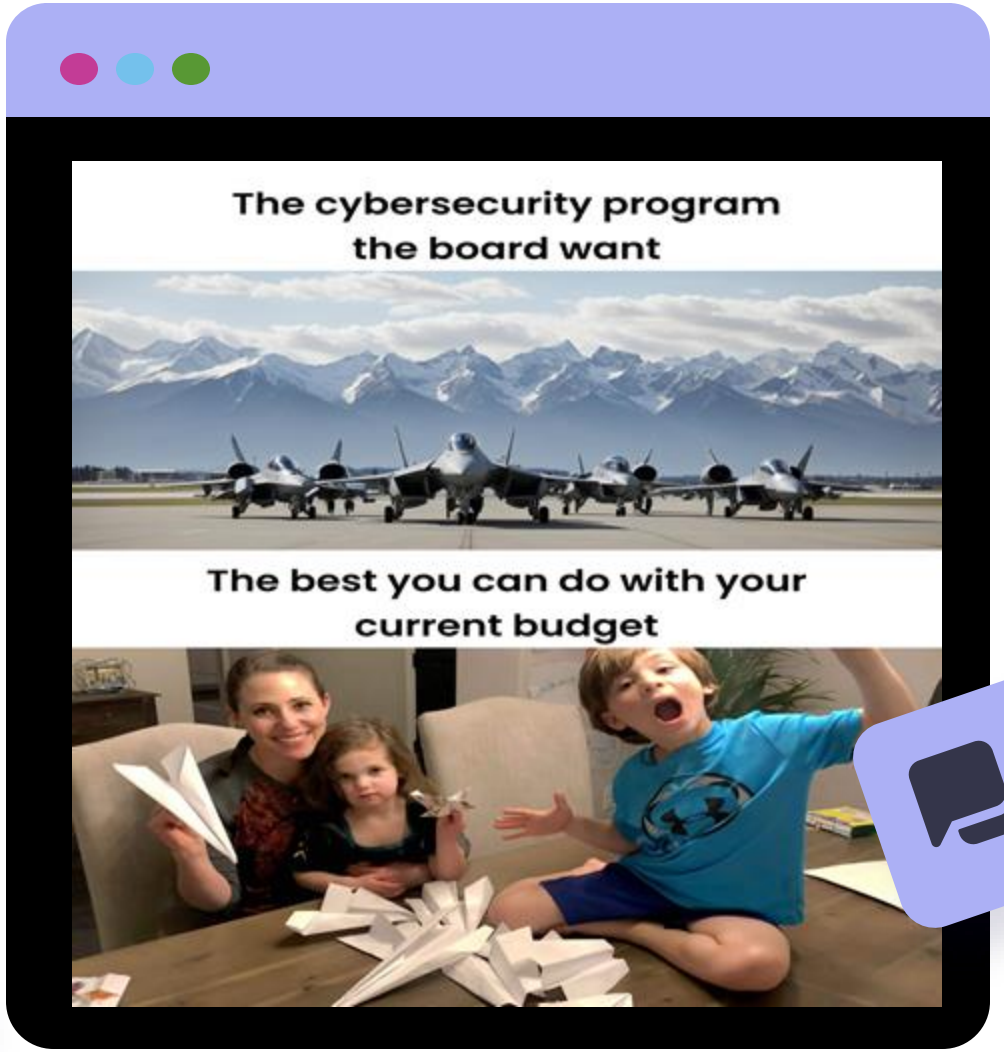



Staff and Compensation Claims the Largest Budget Share

*Breakdown of the annual security budget, 2024*

Sources : 2024 Security Budget Benchmark Report: Key Findings - IANS & Artico Research

# Prioritizing Cybersecurity Spending



# Budget Levers
## at your disposal

# Budget Levers at your disposal

01 Prioritize Spending (80:20 Rule works)

02 Leverage What You Already Have

03 Make your problem, everybody's problem

04 Automate to Save Time and Money

05 Outsource Smartly: Managed Security Services

06 Master the art of Vendor Negotiation

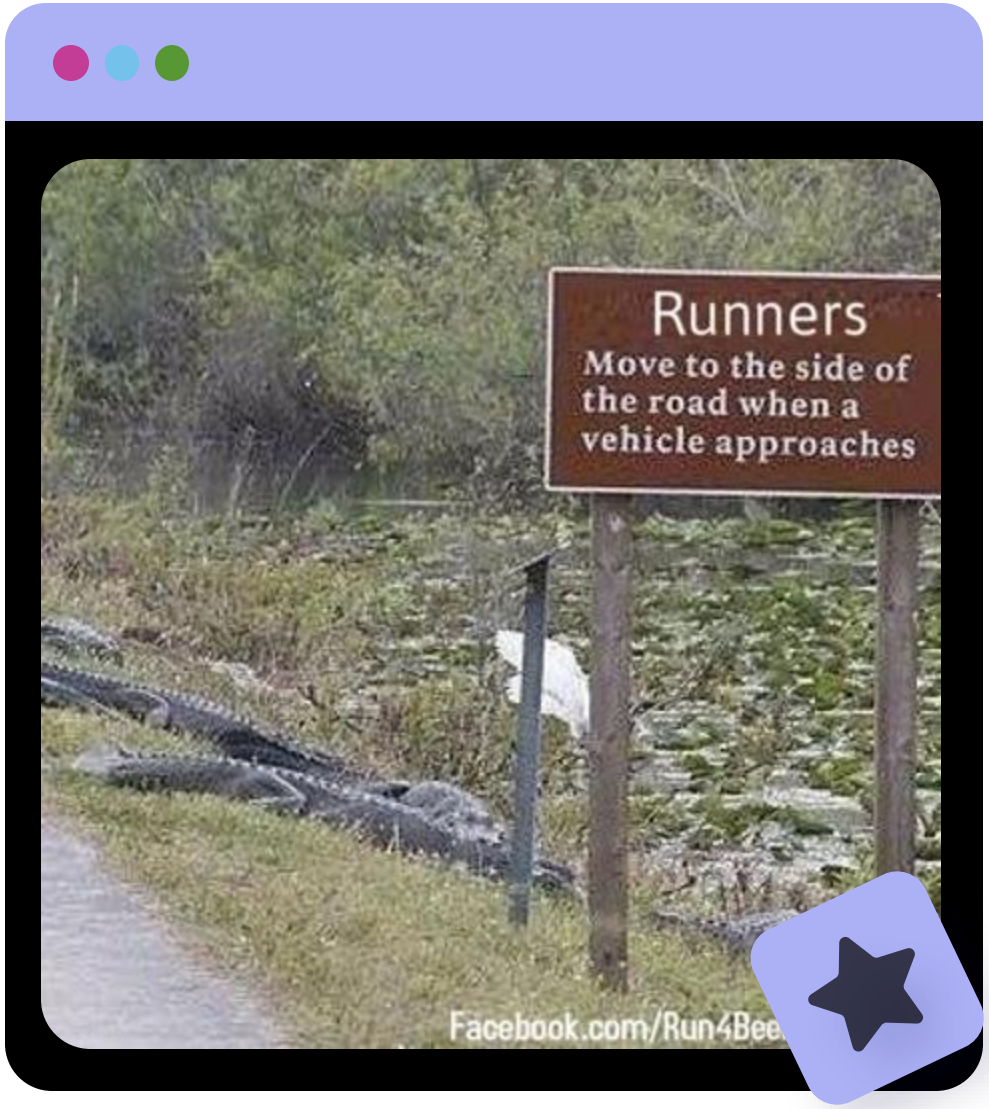
07 Utilize Open-Source / Free Tools

08 Transfer Risk using Cyber Insurance

# Best Practices Are Situational

Best practices depend entirely on your situation

When evaluating whether to apply a "best practice" make sure you understand how it applies to you.



# 01 Prioritize Spending on the 20% that gives 80% returns

- **Compliance Centered Approach (Get out of jail card)** - Map all Standards/Regulations/Laws to processes/controls and target the cost-effective way to comply
- **Asset Centered Approach (Crown Jewels)** - Prioritize spend on the business critical apps, IP Protection, PII/PHI etc.
- **Vulnerability Centered Approach** - Not all Vulnerabilities are equal. Apply internal knowledge on the published CWE/CVEs to prioritize the truly reachable/exploitable vulnerabilities.
- **CIS Top 18** - Leverage CIS (Center for Internet Security) Controls to implement 80:20 rule within the Controls Posture.
- **Loss Centered Approach** - Use your operational loss data, historical data breach costs and actuarial data from cyber insurers to quantify cyber risk in $$$. - FAIR (Factor Analysis of Information Risk)
- **Threat/Risk Centered Approach** - Use threat intelligence (CTEM / ASM) to identify assets that are actively targeted by attackers or most recent incidents

**Other Useful Resources:** MITRE ATT@CK pathways, Penetration test results, ISACs

# 02 Leverage What You Already Have

A typical Enterprise has 76+ Security Products in their Security environment. Focus on ways to maximize current tools, talent, and processes first, before looking at new purchases.

## Maximize ROI on current tools

Perform a Maturity Assessment and Security Capability mapping to further consolidate vendors and tools to eliminate redundancy and inefficiency. Ensure every tool demonstrates a clear ROI, which might manifest as labor savings, threat mitigation, or operational impact.

## Optimization Strategies

| | |
|---|---|
| Improve integration across decentralized security tools for **unified policy enforcement** and threat visibility (CSMA) | Leverage RPA, SOAR or **hyper-automation** tools towards labor savings |
| Review misconfigurations and fix it periodically (e.g. Firewall Rule Reviews) | Maximize Existing Cloud-Native Security Controls (Azure Defender, AWS GuardDuty, Google Security Command Center) |
| Leverage full capabilities of the tools you are already paying for | Tune SIEM & XDR Correlation & Alert Rules (If you have in-house SOC/SIEM) |
| Eliminate overlapping capabilities where you are paying extra (Every vendor is a platform nowadays) | Leverage Microsoft Defender and Purview DLP is you already have an E5 license. |

# 02 Leverage What You Already Have (cont…)

## Optimization Strategies

| |
|---|
| Use an **All-in-one platform** if you are small enough (Startup/SMB/Mid-market) |
| **Optimize SIEM Logs:** Consider reducing unnecessary log ingest through capabilities like Cribl |
| **Automate Patch Management & Compliance Monitoring:** Use **existing VM & endpoint tools** for automated remediation. |
| **Consolidate Dashboards:** Integrate data from multiple tools into a single dashboard to make better use of current monitoring systems. |
| **Enforce Zero Trust Principles:** Use **existing IAM, network segmentation, and micro-segmentation capabilities** to limit lateral movement. |
| **Use Built-In Threat Feeds:** Many tools come with embedded threat intelligence. Ensure these are actively used to inform defense strategies. |
| Invest in cross-training of resources to better contain threats |
| **Shift Left on Security Engineering:** Embed security earlier in **DevSecOps pipelines** using existing **SAST/DAST/IAST capabilities**. |

# 03 Make your problem, everybody's problem

## Align Cybersecurity with Business Goals

- ❑ Keywords: Strategic driver, trust, ROI

## Have the Board on your Speed dial

- ❑ Tabletops, Cyber Risk, personal liability

## Foster Cross-Departmental Collaboration

- ❑ Keywords: Secure by Design, Patching, Legal & Compliance

## Influence your Third/Fourth Parties

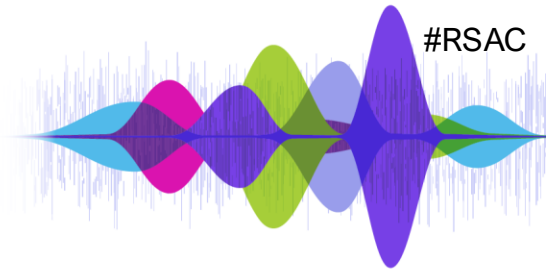
- ❑ Contracts, weakest link, continuous posture

## Create a Security Champions Program

- ❑ Keywords: Human Firewall, Everyone is a risk manager

## Influence your Customers

- ❑ Customer Tools, Awareness, Best Practices



# 04 Automate to Save Time and Money

| Projects | Capability | Tools |
|---|---|---|
| **01** **Automate Log Collection and Analysis with SIEM Tools** | Automate the collection, analysis, and correlation of security event logs to detect threats in real time. | Leverage free or affordable tools like **Elastic** SIEM, **Splunk Free,** or **Graylog** to centralize log data from various systems and automate detection of anomalies without expensive manual monitoring. |
| **02** **Automate Patch Management** | Automate the scanning and patching of vulnerabilities to keep systems updated without manual intervention. | Use free or low-cost tools like **WSUS** (Windows Server Update Services) for Windows environments or **Automox** for cross-platform automated patch management, which saves time and reduces human error. |
| **03** **Automate Vulnerability Scanning and Remediation** | Automatically scan for vulnerabilities and provide actionable remediation steps on a regular schedule. | Utilize tools like OpenVAS or Tenable Nessus Essentials (free for small environments) to run continuous vulnerability scans and generate reports. |

# 04 Automate to Save Time and Money

| Projects | Capability | Tools |
|---|---|---|
| 04 **Automate Phishing Detection and Response** | Automate the detection of phishing attempts and the response process to minimize manual intervention. | Implement tools like **Cofense Triage or PhishER**, which can integrate with your email system to detect, report, and automatically respond to phishing threats without consuming human resources. |
| 05 **Automated Endpoint Detection and Response (EDR)** | Automate threat detection and response on endpoints to identify and neutralize threats without manual monitoring. | Deploy budget-friendly or free solutions like **OSSEC** (open-source) or **Cynet** (offers free versions for small teams) to automate the detection and remediation of endpoint threats. |
| 06 **Automate Incident Response Playbooks** | Implement automated workflows for incident response to standardize processes and reduce response time. | Use orchestration and automation platforms like **TheHive or Shuffle** (open-source SOAR) to automate incident response playbooks and alerting, which helps speed up response without relying on large teams. |

05

# Outsource Smartly: Managed Security Services

- **Managed SOC / MDR:** Outsource 24/7 threat monitoring and incident response to MSSPs, reducing the need for costly in-house infrastructure and expertise.
- **VMaaS & PenTestaaS**: External experts provide unbiased, up-to-date vulnerability assessments and penetration testing at lower costs.
- **Digital Forensics & Incident Response (DFIR)**: Outsourcing ensures quick, specialized incident containment and recovery, and coordination with law enforcement and cyber insurers
- **Identity Threat Detection & Response (ITDR)**: 24/7 identity monitoring focussed on Session hijacking, Credential theft, Account takeover and business email compromise (BEC) attempts
- **Managed Security Awareness**: Deliver continuous and annual security awareness campaigns and tailored trainings
- **vCISO**: External compliance experts ensure regulatory adherence and perform audits, saving internal resources and reducing risk.

# 06 Master the art of Negotiating Better Deals with Vendors

## Do Thorough Market Research

- Understand the market, features, and competitors.
- Have alternative vendors and a clear knowledge of the pricing landscape.
- Analysts like Gartner, Forrester or G2 Crowd can help.
- Partnering with a Value Added Reseller (VAR)

## Ask for Flexibility in Pricing Models

- Explore Leasing options to convert Capex to Opex
- Negotiate for flexible payment plans, pay-as-you-go options, or usage-based pricing
- SaaS subscriptions can be sneaky. Evaluate on case-by-case basis

## Long-Term Partnership Opportunities

- Position your organization as a potential long-term partner. Vendors are often more willing to negotiate if they see opportunities for upsell, referrals, or long-term collaboration.

## Bundle Multiple Solutions for Discounts

- If a vendor offers multiple products or services, try to bundle them together for a bulk discount.
- Additionally, explore longer-term contracts for lower pricing.

## Leverage Trials and POVs

- Ask for free trials or PoVs before committing. Use the trial period to demonstrate the value to your organization.
- Positive PoV results can get better terms, as vendors want to convert trials into long-term contracts.

## Negotiate Maintenance and Support Costs

- Negotiate lower or bundled maintenance/support costs and explore a tiered support plan.
- VaRs often have better pricing on First Call Support and professional services support than vendors.

# 07 Utilize Open-Source / SMB Friendly Tools

## Cloud Security

- **CloudSploit by Aqua Security** is a functional, CSPM that is pretty low lift to get up and running to audit various public cloud providers.
- **Cloud Custodian:** Policy-as-code tool for managing cloud security posture.

## Network Security

- **Snort / Suricata /Security Onion** are Free open source network intrusion detection system (IDS) and intrusion prevention system (IPS).
- **Wireshark** is a Network protocol analyzer for troubleshooting and analysis.
- **OpenVPN** - Secure remote access using VPN tunnels.
- **Let's Encrypt** - free SSL/TLS certificates to secure websites.
- **Nmap:** Network scanner for identifying vulnerabilities and open ports

## EndPoint Security / Vuln Mgmt

- **ClamAV:** Open-source antivirus and malware scanner.
- **OSSEC:** Host-based intrusion detection system (HIDS) for monitoring endpoints.
- **OpenVAS :** Comprehensive vulnerability scanning and management
- **Nikto:** Web server scanner to identify outdated and vulnerable configurations.

## Application Security

- **OWASP ZAP (Zed Attack Proxy):** Web application security testing.
- **Burp Suite:** Basic web vulnerability scanning and testing.
- **Bandit:** Static application security testing (SAST) for Python code.

## Threat Intelligence

- Use free or low-cost threat intelligence services like **AlienVault Open Threat Exchange (OTX), MISP, MITRE ATT&CK** to stay updated on emerging threats and adjust your defense strategy accordingly.

## Security Operations

- If you're willing to deploy a dedicated SIEM, consider **Wazuh** as an open-source solution
- **Elasticsearch, Logstash, and Kibana** (ELK Stack): Log collection, search, and visualization for security monitoring.
- **Graylog**: Centralized log management and analysis.

Source: https://ventureinsecurity.net/

# 08 Cyber Insurance

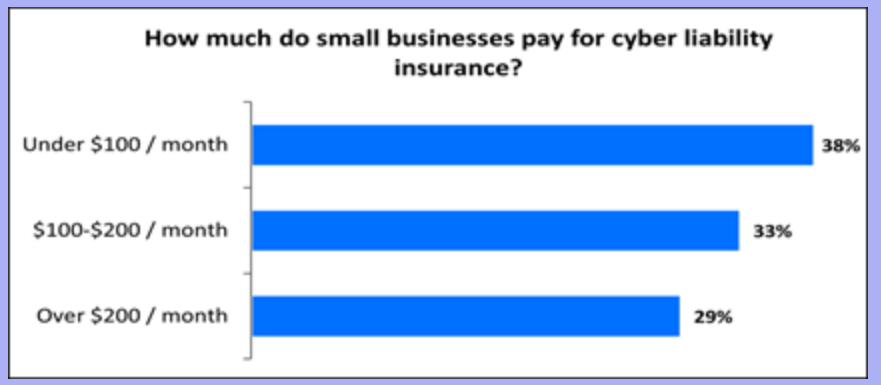
By combining cyber insurance with strategically selected security investments like, endpoint protection, backups, and employee training, businesses can build a cost-effective security program.

Instead of investing randomly in every possible defense, one can focus on risks uncovered by Inusrance or mandated by insurance and rely on insurance to offset rare, but financially devastating events (e.g. APT, Ransomware, DDoS). Optimize your security investments in line with insurance requirements to qualify for **lower premiums**.

## Cyber insurance can play a good part in a budget-friendly cyber security strategy:

Coverage of Financial Losses like Breach Response costs, claims by third-parties and any interruptions caused to business operations due to breach. Typical coverage is from $1-5M which partially covers costs of a Data Breach.

Insurance Premium depends on factors such as amount of sensitive data, business revenues, no. of employees with access, types of services, and prior claims history to name a few.




Risk Transfer Strategy: Budget-conscious security initiatives often find it difficult to implement each and every security measure due to limited funds. In such cases, Cyber insurance helps transfer part of the financial risk to the insurer. Also, these insurers often require certain baseline security measures (e.g., firewalls, encryption, incident response plans) before offering coverage which can in turn drive organizations to improve security.

*Disclaimer: Cyber insurance should not be considered in place of effective and robust cyber risk management. All companies need to purchase cyber insurance but should only consider it to mitigate the damage caused by a potential cyber attack.*

# Bonus Ideas!

**a**

**Free Cyber Risk Assessments**

**b**

**Strategic Alliances & Information Sharing**

**c**

**Secure Layer 8 (Humans)**

**d**

**Cyber Risk Quantification**

a

# Free Cyber Risk Assessments

Many security vendors provide free tools, assessments, or trial versions to help organizations understand their risks and improve their security posture

01 Use Free Tools from Vendors for Risk and Compliance Assessments

02 Leverage Free Trials for Advanced Features

03 Request Vendor-Led Assessments

04 Use Open-Source Tools Sponsored by Vendors

| | |
|---|---|
| **Compliance** | Free compliance readiness checks for SOC 2, ISO 27001, and GDPR. (SecureFrame, CyberSaint, Drata etc.) |
| **Vulnerabilities** | Free trial for vulnerability scanning and risk assessment. (Qualys Community Edition). Utilize free tools like OWASP Risk Assessment Framework or Microsoft's Security Assessment Tool (MSAT). |
| **Third Party Security Ratings** | Free vendor risk and self-risk assessment for a limited time. (BitSight, Security Scorecard) |
| **Firewall Review** | Free risk assessment report using existing Palo Alto firewalls. (Palo Alto Networks Security Lifecycle Review, FireMon Policy Analyzer) |
| **CSPM / ASPM / DSPM** | Free cloud assessments for AWS (AWS Well-Architected Tool) and Azure (Microsoft Secure Score) and Data Risk Assessments (Varonis) |
| **Vendor-Led Assessments** | Free Cloud Security Review (Checkpoint CloudGuard Dome9 Free Assessment)<br>Free Threat Hunting (CrowdStrike Security Assessment) |

b

# Building Strategic Alliances for Shared Cybersecurity Resources

Discuss partnerships with industry groups or alliances that offer shared security resources.

## Industry Groups/Agencies

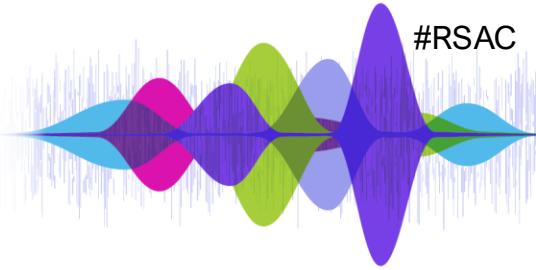
- ✓ **CISA (Cybersecurity and Infrastructure Security Agency):** Threat intelligence sharing (e.g., JCDC, Shields Up).
- ✓ **FBI InfraGard:** Trusted info-sharing with private sector.
- ✓ **ISACs/ISAOs (e.g., FS-ISAC, H-ISAC):** Sector-specific cyber threat exchange.
- ✓ **NCCoE (NIST National Cybersecurity Center of Excellence):** Collaborative projects, implementation guidelines.

## Collaborative Platforms

- ✓ **MITRE ATT&CK & Engage:** Open knowledge base for adversary tactics; engagement frameworks.
- ✓ **FIRST (Forum of Incident Response and Security Teams):** Coordination and response support.
- ✓ **OpenSSF / OWASP:** Shared tools and standards for software & app security.

## Strategic Benefits

- ✓ **Shared threat intelligence → Faster detection & response**
- ✓ **Reduced costs through pooled resources & tooling**
- ✓ **Enhanced credibility and regulatory alignment**
- ✓ **Stronger collective defense posture**



C

# Invest in Cybersecurity Culture (Secure Layer 8)

Humans contribute to more than 50% of cyber risk.

| Provider | Resource Name | Link |
|---|---|---|
| **CISA** | CISA Cybersecurity Awareness Training | https://www.cisa.gov/cybersecurity-training-exercises |
| **National Cyber Security Alliance (NCSA)** | Cybersecurity Awareness for Employees | https://staysafeonline.org/ |
| **Federal Trade Commission (FTC)** | Cybersecurity for Small Businesses | https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity |
| **Global Cyber Alliance (GCA)** | Cybersecurity Toolkit for Small Businesses | https://gcatoolkit.org/ |
| **UK National Cyber Security Centre (NCSC)** | Small Business Training | https://www.ncsc.gov.uk/cyberaware |
| **SANS Institute** | SANS Cyber Aces | https://www.cyberaces.org/ |
| **IBM Security Learning Academy** | Employee Security Awareness Modules | https://www.securitylearningacademy.com/ |
| **KnowBe4** | Security Awareness Training (Free Version) | https://www.knowbe4.com/ |
| **Cybersecurity & Infrastructure Security Agency (CISA)** | Phishing Awareness Training | https://www.cisa.gov/cybersecurity-training-exercises |
| **Department of Defense (DoD)** | Cyber Hygiene Training | https://public.cyber.mil/ |
| **National Institute of Standards and Technology (NIST)** | NICE Cybersecurity Learning Content | https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content |

# d Quantifying Cyber Security ROI

## The True Costs of a Security Breach

A common formula is:

**Cybersecurity ROI = (Benefits – Costs) / Costs x 100%**

Benefits: Total value gained from cybersecurity initiatives - can include money saved from avoiding breaches, reduced risk levels, or any financial gains.

Costs: Total expenses incurred to implement cybersecurity strategies - including cost of software, hardware, training, and any other resources needed.

This percentage reflects the efficiency of cybersecurity investments, showing how much benefit is received for each dollar spent.

ROI of investing in cybersecurity: Comparing the cost of the said preventative measure against the cost of potential breaches it prevents.

Direct costs like fines, legal fees and indirect costs like reputational damage and loss of customer trust should also come while calculating potential damages.

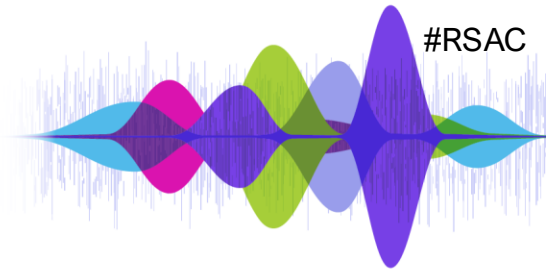
# Key Tactical Next-Steps!

# If you took nothing else from this talk, take the following 8 tactical measures at the very least.

# Top Recommendations to Optimize Budget

Here are 8 top recommendations for maximizing ROI, reclaiming budget from tech debt, and optimizing investments

| Budget Lever | Key Insight | Action |
|---|---|---|
| Prioritize Spending Using the 80/20 Rule | 20% of security investments provide 80% of the protection. | • Focus on protecting business-critical assets, prioritizing risk-based budgeting, and investing in security controls with the highest impact (e.g., MFA, endpoint detection, patching automation). |
| Leverage What You Already Have | Enterprises have an average of **76 security tools**, many of which are redundant. | • Conduct a **security tool rationalization exercise** to consolidate solutions, eliminate overlapping technologies, and renegotiate contracts. |
| Make Cybersecurity a Shared Responsibility | Cybersecurity should not be a cost center—it should be seen as an enabler of business resilience. | • Partner with functional leaders (IT, DevOps, Legal, Finance) to **co-fund security initiatives** that benefit multiple teams. |
| Automate to Save Time and Money | Security teams are overwhelmed with alerts and manual processes. | • Invest in **automation for log management, vulnerability scanning, phishing detection, and incident response**. |
| Outsource Smartly with Managed Security Services | Not all security functions need to be in-house. | • **Outsource 24/7 SOC, MDR, and penetration testing** to managed service providers for cost efficiency. |
| Become a Master Negotiator | Many organizations **overpay for security solutions** due to lack of price benchmarking | • **Renegotiate contracts** with volume discounts or bundled solutions. **Leverage free trials and open-source tools** before committing to expensive solutions. **Utilize VARs (Value-Added Resellers)** to access group pricing and alternative solutions. |
| Utilize Open-Source and Free Security Tools | Open-source and SMB focused security tools offer near enterprise-grade capabilities at minimal cost. | • Use **ClamAV** or **Microsoft Defender** for malware protection, **OpenVAS** for vulnerability scanning, etc. |
| Transfer Risk Using Cyber Insurance | Cyber insurance can mitigate financial losses from ransomware and data breaches. | • Optimize your **security investments in line with insurance requirements** (e.g., MFA, backup policies) to qualify for lower premiums. |



# Must-Have Security

Any business handling confidential customer data should have the following at the very least.

| Security Domain | Justification | Suggested Measures |
|---|---|---|
| Identity & Access Management (IAM) | Prevent unauthorized access to critical systems. | • Implement **Multi-Factor Authentication (MFA)** (NIST 800-63, CIS Control 6, CISA Zero Trust Guidance).<br>• Enforce **least privilege** and **role-based access control (RBAC)** (CIS Control 5, NIST 800-53 AC-6).<br>• Use **Single Sign-On (SSO)** and monitor privileged accounts. |
| Endpoint Protection & Device Security | Protect against malware, ransomware, and unauthorized access. | • Deploy **Endpoint Detection & Response (EDR)** or **Next-Gen Antivirus (NGAV)** (CIS Control 10, CISA Ransomware Guide).<br>• Enforce **full-disk encryption** for laptops and mobile devices (NIST 800-111, CIS Control 14).<br>• Implement **Mobile Device Management (MDM)** for remote security. |
| Network & Perimeter Security | Prevent unauthorized access and lateral movement in the network. | • Deploy **firewalls (NGFW) and Intrusion Detection/Prevention Systems (IDS/IPS)** (CIS Control 13, NIST 800-41).<br>• Use **Zero Trust Network Access (ZTNA) or VPN** for remote access (CISA Zero Trust Maturity Model).<br>• Enforce **Wi-Fi security** (WPA3 where possible). |
| Email & Phishing Protection | Email is the top attack vector for ransomware and phishing. | • Use **Secure Email Gateway (SEG) or cloud-native email security** (CIS Control 9, CISA Phishing Guidance).<br>• Implement **DMARC, DKIM, SPF** to prevent email spoofing (CISA StopRansomware Guide).<br>• Conduct **employee phishing training and simulations**. |
| Data Protection & Backup Strategy | Protects sensitive data and ensures recovery from cyber incidents. | • Enforce **Data Loss Prevention (DLP) policies** (CIS Control 3, NIST 800-53 MP-5).<br>• Implement **immutable, air-gapped backups** and regularly test restoration (CISA Ransomware Recovery Guide).<br>• Apply data minimization and data masking strategies to reduce the need to collect or obfuscate data.<br>• Encrypt **data at rest and in transit** (CIS Control 14, NIST 800-175B). |

# Must-Have Security

| Security Domain | Justification | Suggested Measures |
|---|---|---|
| Security Monitoring & Incident Response | Enables early detection and swift response to threats. | • Implement **Security Information & Event Management (SIEM)** or **SOC** (CIS Control 8, NIST 800-92).<br>• Have an **Incident Response Plan (IRP)** with tested playbooks (NIST 800-61, CISA Incident Response Guide).<br>• CISA proposes maintaining accurate network topology for effective incident identification and response.<br>• Enable **24/7 monitoring via a SOC or MDR provider**. |
| Vulnerability & Patch Management | Addresses exploitable weaknesses before attackers can. | • Maintain and update an **asset inventory** every month, including IP addresses and hardware MAC addresses.<br>• Conduct **regular vulnerability scanning and remediation tracking** (CIS Control 7, CISA Known Exploited Vulnerabilities Catalog).<br>• Automate **patch management** for OS, apps, and firmware (NIST 800-40, CIS Control 7).<br>• Remediate known exploited vulnerabilities (KEVs) within 14 days & high-severity CVEs in 30 days. |
| Security Awareness & Governance | Employees are the first line of defense against cyber threats. | • Conduct **regular cybersecurity awareness training** (CIS Control 14, NIST 800-50).<br>• Develop and enforce **security policies** (e.g., password management, remote work) (NIST CSF PR.AT-1).<br>• Align with **industry standards (NIST CSF, CIS Controls, ISO 27001, CISA best practices)**. |
| Cloud Security * | Protects cloud workloads, data, and identities from evolving threats in shared responsibility environments. | • **Cloud Security Posture Management (CSPM):** Continuously monitor cloud misconfigurations and enforce compliance (CIS Control 4, NIST 800-53 CM-6, CISA Cloud Security Guidance).<br>• **Cloud Identity & Access Management (CIAM):** Enforce **least privilege, role-based access, and conditional access** (CIS Control 5, NIST 800-53 AC-2, CISA Zero Trust Guidance).<br>• **Cloud Workload Protection Platform (CWPP):** Secure **VMs, containers, and serverless functions** against runtime threats (NIST 800-190, CIS Control 10). |
| Application Security * | Prevents security vulnerabilities in software and web applications that could be exploited by attackers. | • **Secure Software Development Lifecycle (SSDLC):** Embed **security in CI/CD pipelines** using static/dynamic application security testing (SAST/DAST) (NIST SSDF, CIS Control 16).<br>• **Application Penetration Testing & Threat Modeling:** Conduct **regular security assessments, red teaming, and threat modeling** (CIS Control 18, NIST 800-115).<br>• **Web Application Firewall (WAF):** Protect against **OWASP Top 10 threats (SQL injection, XSS, CSRF, etc.)** (CIS Control 13, CISA Web App Security Guidance).<br>• **Secure API Development & Gateway Protection:** Enforce **OAuth 2.0, API rate-limiting, and authentication mechanisms** (NIST 800-204, CIS Control 4). |

# Off Limits Solutions for Frugal CISOs

Solutions most underfunded orgs shouldn't pursue. These only provide marginal benefit unless you are an Enterprise that is specifically targeted by Advanced Persistent Threats (APTs) and has a range of maturity levels due to multiple mergers and acquisitions.

01 In-house SOC or XDR

02 Premium Threat Intel feeds

03 Fancy "ransomware prevention" tools

04 Blockchain for Security

05 Breach & Attack Simulation /Continuous PenTesting

06 Quantum resistant Cryptography

07 Gamified security awareness training

08 AI / Autonomous SOC Analysts

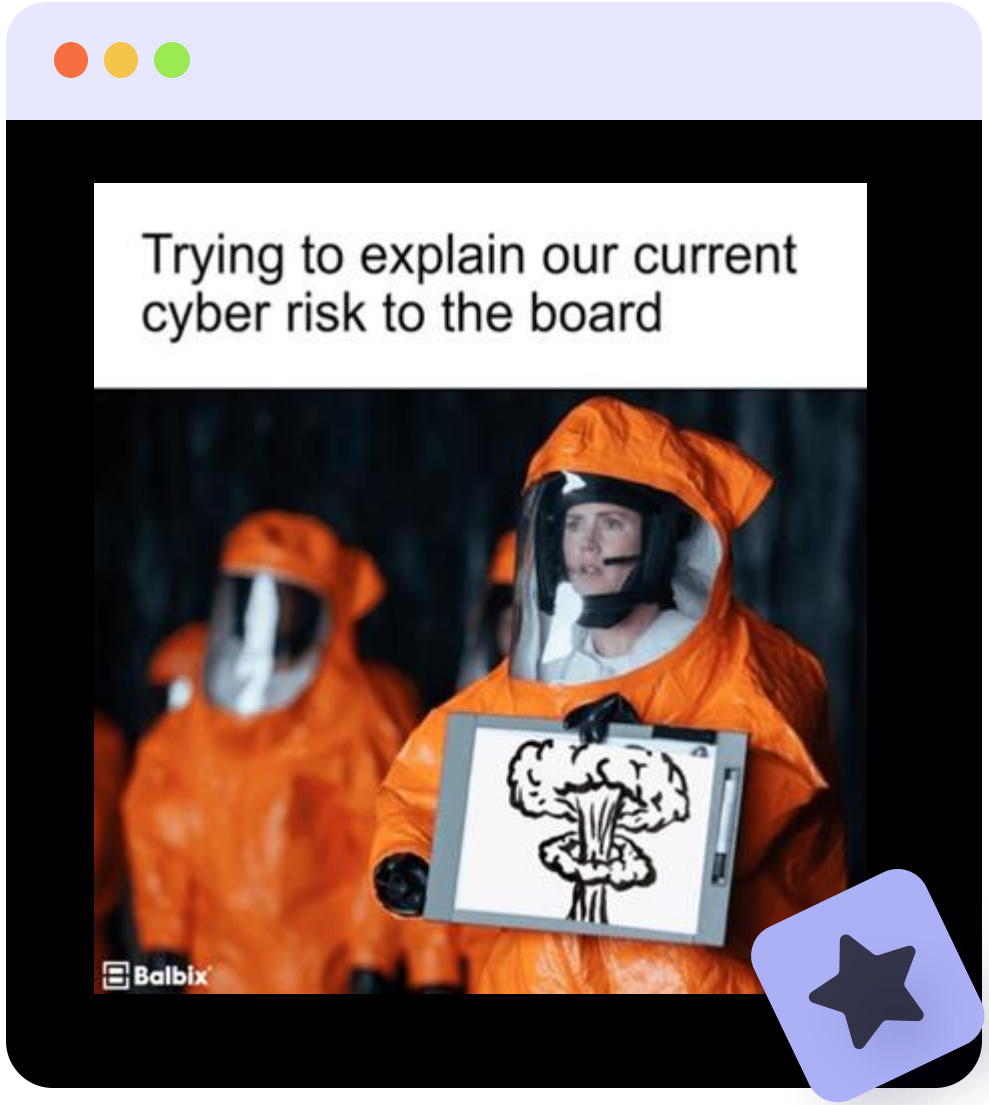
09 Deception Technology – Honeypot/Decoy/Tripwires

10 Premium Insider Threat Solutions

# Apply what you learned today

- **Next week you should:**
  - Pick a security domain (identity, data etc.) and leverage one of the Free assessments covered in the talk to assess the security posture / maturity.
  - Kick-off an Asset Inventory refresh, identify crown jewels and automate the process ***(you cannot defend or protect what you do not know )***
- **In the first three months following this presentation you should:**
  - Ensure your Security Plan and Incident Response Plan is accurate and get it approved by the Board.
  - Engage with your VAR/Solutions Partners to perform tools rationalization and develop a roadmap focused on optimization and efficiency gains **(often there is money to be reclaimed from tech debt)**
- **Within six months you should:**
  - Create a formal program/project to optimize the people, process and technology for the chosen Security Domain **(Fix your critical/high issues related to People and Process first, before committing to more technology.)**

# Questions ?


Trying to explain our current cyber risk to the board
Balbix

CYBER SECURITY BUDGET BEFORE A BREACH
CYBER SECURITY BUDGET AFTER A BREACH

# Thank you

Anand Thangaraju

*Field CISO, Board Director, Investor,*
*VC Catalyst, Speaker*

RSAC 2025 Conference

RSAC 2025 Conference

Many Voices.
**One Community.**

**Anand Thangaraju**

Field CISO, Board Director, Investor,

VC Catalyst, Speaker